Bound entangled states with nonzero distillable key rate

Dong Pyo Chi,[1,*] Jeong Woon Choi,[1,†] Jeong San Kim,[1,‡] Taewan Kim,[1,§] and Soojoon Lee[2,¶]

[1] *Department of Mathematical Sciences, Seoul National University, Seoul 151-742, Korea*
[2] *Department of Mathematics and Research Institute for Basic Sciences, Kyung Hee University, Seoul 130-701, Korea*

(Dated: February 13, 2007)

In this paper, we present sufficient conditions for states to have positive distillable key rate. Exploiting the conditions, we show that the bound entangled states given by Horodecki *et al.* [Phys. Rev. Lett. **94**, 160502 (2005), quant-ph/0506203] have nonzero distillable key rate, and finally exhibit new classes of bound entangled states with positive distillable key rate, but with negative Devetak-Winter lower bound of distillable key rate for the ccq states of their privacy squeezed versions.

PACS numbers: 03.67.-a, 03.65.Ud, 03.67.Mn, 03.67.Hk

I. INTRODUCTION

Quantum cryptography provides us with a perfectly secure cryptosystem, which is feasible in a practical way as well as in a theoretical way. In particular, quantum key distribution among quantum cryptographic protocols can be considered as one of the most important applications of quantum entanglement, since secure key distillation in quantum key distribution is closely related with entanglement distillation [1, 2].

It has been known that there are two different types of entanglement. One is called the *free* (or, *distillable*) entanglement, from which one can distill a pure entanglement useful for quantum communication by local quantum operation and classical communication (LOCC), and the other is called the *bound* (or, *nondistillable*) entanglement, which is not distillable. Even though one cannot distill a pure entanglement useful for quantum communication from the bound entanglement, it has been shown that any bound entangled states can be useful in quantum teleportation [3, 4]. Recently, Horodecki *et al.* [6, 7, 8] have shown that there are some classes of bound entangled states with positive key rate by showing that the lower bound K_D^{DW} of distillable key rate introduced in [5] is more than zero for those states.

However, the question of whether every entangled state has positive distillable key rate, $K_D > 0$, has still remained open. In this paper, we investigate the properties of quantum states with nonzero distillable key rate, and construct several sufficient conditions of $K_D > 0$. Exploiting the conditions, we show that the bound entangled states with positive partial transpose (PPT) given in [6, 7, 8] have nonzero distillable key rate, and finally present a new class of PPT bound entangled states satisfying $K_D > 0$, although $K_D^{DW} < 0$ for the ccq states of their privacy squeezed versions presented in [7, 8].

This paper is organized as follows. In Sec. II we recall the concepts of private states and distillable key rate in [7]. In Sec. III we construct the sufficient conditions for states with $K_D > 0$. In Sec. IV we show that the PPT bound entangled states given in [6, 7, 8] have nonzero distillable key rate, and exhibit new classes of PPT bound entangled states satisfying $K_D > 0$, but $K_D^{DW} < 0$ for the ccq states of their privacy squeezed versions. Finally, in Sec. V we summarize our results.

II. PRIVATE STATES AND DISTILLABLE KEY RATE

For a positive integer $d \geq 2$, a *private state* (or, *pdit*) $\gamma_{ABA'B'}$ on $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_{B'}}$ with $d_A = d_B = d$, is defined as $\gamma_{ABA'B'} = U\left|\psi_d^+\right\rangle\left\langle\psi_d^+\right| \otimes \rho_{A'B'}U^\dagger$, where

$$\left|\psi_d^+\right\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|kk\rangle_{AB}, \tag{1}$$

$\rho_{A'B'}$ is an arbitrary state of the subsystem $A'B'$, and U is an arbitrary twisting operation

$$U = \sum_{k,l=0}^{d-1}|kl\rangle\langle kl| \otimes U_{kl} \tag{2}$$

with unitary matrices U_{kl}. Then $\gamma_{ABA'B'}$ can be rewritten as

$$\gamma_{ABA'B'} = \frac{1}{d}\sum_{k,l=0}^{d-1}|kk\rangle\langle ll| \otimes U_{kk}\rho_{A'B'}U_{ll}^\dagger. \tag{3}$$

When $d = 2$, $\gamma_{ABA'B'}$ is called a *private bit* (or, *pbit*). Then we can have the following proposition [7].

Proposition 1. *If a state* $\rho \in \mathcal{B}(\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^d\otimes\mathbb{C}^{d'})$ *with* $\rho = \sum_{i,j,k,l}|ij\rangle\langle kl| \otimes A_{ijkl}$ *fulfills* $\|A_{0011}\| \geq 1/2-\varepsilon$, *then for* $0 < \varepsilon < 1$ *there exists a pbit* γ *such that* $\|\rho - \gamma\| \leq$

*Electronic address: dpchi@math.snu.ac.kr
†Electronic address: cju@snu.ac.kr
‡Electronic address: freddie1@snu.ac.kr
§Electronic address: april02@snu.ac.kr
¶Electronic address: level@khu.ac.kr

$\delta(\varepsilon)$ *with* $\delta(\varepsilon)$ *vanishing, when* ε *approaches zero. More specifically,*

$$\delta(\varepsilon) = \sqrt{\ln 2 \left(8\sqrt{2\varepsilon} + h(2\sqrt{2\varepsilon})\right)} + 2\sqrt{2\varepsilon}, \tag{4}$$

where h *is the binary entropy function.*

Now, we define the *distillable key rate* K_D as presented in [7]. Let ρ_{AB} be a given state in $\mathcal{B}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$. For each positive integer n, consider a sequence P_n of LOCC operations such that $P_n(\rho_{AB}^{\otimes n})$ is a state in $\mathcal{B}(\mathbb{C}^{d_n} \otimes \mathbb{C}^{d_n})$. The family of the operations $\mathcal{P} \equiv \{P_n : n \in \mathbb{N}\}$ is called a *pdit distillation protocol* of ρ_{AB} if

$$\lim_{n\to\infty} \|P_n(\rho_{AB}^{\otimes n}) - \gamma_{d_n}\| = 0, \tag{5}$$

where γ_{d_n} is a pdit whose AB part is of dimension d_n^2. The *rate of a protocol* $\mathcal{P}$ is given by

$$R_{\mathcal{P}} = \limsup_{n\to\infty} \frac{\log d_n}{n}, \tag{6}$$

and the *distillable key rate* of ρ_{AB} is defined as the maximum rate of a protocol

$$K_D(\rho_{AB}) = \sup_{\mathcal{P}} R_{\mathcal{P}}. \tag{7}$$

Then the following proposition for the distillable key rate K_D can be obtained, as shown in [7].

Proposition 2. *If a state* ρ *is close enough to a pbit in trace norm, then* $K_D(\rho) > 0$.

III. SUFFICIENT CONDITIONS FOR POSITIVE DISTILLABLE KEY RATE

Proposition 2 in Sec. II provides us with a simple sufficient condition of $K_D(\rho) > 0$, as follows.

Lemma 1. *If one can transform, by LOCC, such as the recurrence protocol, sufficiently many copies of a state* ρ *into a state close enough to a private state in trace norm, then* $K_D(\rho) > 0$.

Proof. Assume that, by LOCC, the state of sufficiently many copies of ρ is transformed into ρ', which is close enough to a pdit in trace norm. Then, by Proposition 2, ρ' has a nonzero distillable key rate, that is, $K_D(\rho') > 0$. Thus, by the definition of K_D, there exists a family of LOCC operations $\mathcal{P}_0$ such that

$$R_{\mathcal{P}_0} = \limsup_{n\to\infty} \frac{\log d_n}{n} \tag{8}$$

is nonzero for ρ'.

Now, let us consider $K_D(\rho)$ in accordance with $K_D(\rho')$. By the assumption, ρ' can be made out of sufficiently many m copies of ρ by LOCC, which is denoted by P'. We let $\mathcal{P} = \{P \circ P' : P \in \mathcal{P}_0\}$. Then $\mathcal{P}$ is a pdit distillation protocol of ρ, and hence we clearly obtain

$$K_D(\rho) \geq R_{\mathcal{P}} = \limsup_{n\to\infty} \frac{\log d_n}{mn} = \frac{R_{\mathcal{P}_0}}{m} > 0. \tag{9}$$

Therefore, this completes the proof. □

By Lemma 1, we have an explicit form of a sufficient condition for $K_D > 0$.

Theorem 1. *Let* ρ *be any state in* $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \otimes \mathbb{C}^d)$ *with* $\rho = \sum_{i,j,k,l=0}^{1} |ij\rangle\langle kl| \otimes A_{ijkl}$. *If* $\|A_{0000}\| = \|A_{0011}\| = \|A_{1111}\|$ *and* $\|A_{0101}\| < \|A_{0011}\|$, $\|A_{1010}\| < \|A_{0011}\|$, *then* $K_D(\rho) > 0$.

Proof. Repeating the recurrence protocol on many copies of ρ, by Lemma 5 in Appendix, we can obtain

$$\rho' = \frac{1}{N} \begin{bmatrix} A_{0000}^{\otimes n} & A_{0001}^{\otimes n} & A_{0010}^{\otimes n} & A_{0011}^{\otimes n} \\ A_{0100}^{\otimes n} & A_{0101}^{\otimes n} & A_{0110}^{\otimes n} & A_{0111}^{\otimes n} \\ A_{1000}^{\otimes n} & A_{1001}^{\otimes n} & A_{1010}^{\otimes n} & A_{1011}^{\otimes n} \\ A_{1100}^{\otimes n} & A_{1101}^{\otimes n} & A_{1110}^{\otimes n} & A_{1111}^{\otimes n} \end{bmatrix}, \tag{10}$$

where $N = \|A_{0000}\|^n + \|A_{0101}\|^n + \|A_{1010}\|^n + \|A_{1111}\|^n$. Then we have $\|A'_{0011}\| = \|A_{0011}\|^n/N$, where A'_{0011} is the upper-right block of ρ'.

Since $\|A_{0000}\| = \|A_{0011}\| = \|A_{1111}\|$, $\|A_{0101}\| < \|A_{0011}\|$, and $\|A_{1010}\| < \|A_{0011}\|$, we can readily show that $\|A'_{0011}\|$ converges to $1/2$ as n tends to infinity. Therefore, by Proposition 1 and Lemma 1, we conclude that $K_D(\rho)$ is positive. □

By Theorem 1, we clearly obtain the following corollary.

Corollary 1. *Let* ρ *be a state in* $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \otimes \mathbb{C}^d)$ *of the form*

$$\begin{aligned} \rho \;=\; & \left|\phi^+\right\rangle\!\left\langle\phi^+\right| \otimes \sigma_0 + \left|\phi^-\right\rangle\!\left\langle\phi^-\right| \otimes \sigma_1 \\ & + \left|\psi^+\right\rangle\!\left\langle\psi^+\right| \otimes \sigma_2 + \left|\psi^-\right\rangle\!\left\langle\psi^-\right| \otimes \sigma_3, \end{aligned} \tag{11}$$

where $|\phi^\pm\rangle$ *and* $|\psi^\pm\rangle$ *are Bell states in* $\mathbb{C}^2 \otimes \mathbb{C}^2$. *Then if* $\|\sigma_0 - \sigma_1\| > 1/2$ *and* $\mathrm{tr}(\sigma_0\sigma_1) = 0$, *then* $K_D(\rho) > 0$.

Proof. ρ has the following matrix form:

$$\rho = \frac{1}{2} \begin{bmatrix} \sigma_0 + \sigma_1 & 0 & 0 & \sigma_0 - \sigma_1 \\ 0 & \sigma_2 + \sigma_3 & \sigma_2 - \sigma_3 & 0 \\ 0 & \sigma_2 - \sigma_3 & \sigma_2 + \sigma_3 & 0 \\ \sigma_0 - \sigma_1 & 0 & 0 & \sigma_0 + \sigma_1 \end{bmatrix}. \tag{12}$$

By Lemma 4 in Appendix, we have $\|\sigma_0 - \sigma_1\| = \|\sigma_0 + \sigma_1\|$, and hence $\|\sigma_2 + \sigma_3\| < 1/2 < \|\sigma_0 + \sigma_1\|$. Therefore, since all the hypotheses in Theorem 1 are satisfied, we conclude that $K_D(\rho) > 0$. □

Now, let us consider the *privacy squeezed* state σ_{AB} of ρ in Eq. (11), which has been introduced in [7, 8], is

$$\sigma_{AB} = \frac{1}{2} \begin{bmatrix} \|\sigma_0 + \sigma_1\| & 0 & 0 & \|\sigma_0 - \sigma_1\| \\ 0 & \|\sigma_2 + \sigma_3\| & \|\sigma_2 - \sigma_3\| & 0 \\ 0 & \|\sigma_2 - \sigma_3\| & \|\sigma_2 + \sigma_3\| & 0 \\ \|\sigma_0 - \sigma_1\| & 0 & 0 & \|\sigma_0 + \sigma_1\| \end{bmatrix}, \tag{13}$$

and let $|\Psi\rangle_{ABE}$ be a purification of σ_{AB}. Then

$$\begin{aligned}|\Psi\rangle_{ABE} &= \sqrt{x}|\phi^+\rangle|e_0\rangle + \sqrt{y}|\phi^-\rangle|e_1\rangle \\ &\quad +\sqrt{z}|\psi^+\rangle|e_2\rangle + \sqrt{w}|\psi^-\rangle|e_3\rangle \\ &= \frac{1}{2}|00\rangle \otimes \left(\sqrt{x}|e_0\rangle + \sqrt{y}|e_1\rangle\right) \\ &\quad +\frac{1}{2}|11\rangle \otimes \left(\sqrt{x}|e_0\rangle - \sqrt{y}|e_1\rangle\right) \\ &\quad +\frac{1}{2}|01\rangle \otimes \left(\sqrt{z}|e_2\rangle + \sqrt{w}|e_3\rangle\right) \\ &\quad +\frac{1}{2}|10\rangle \otimes \left(\sqrt{z}|e_2\rangle - \sqrt{w}|e_3\rangle\right), \end{aligned} \quad (14)$$

where

$$\begin{aligned} x &= \frac{1}{2}\left(\|\sigma_0+\sigma_1\| + \|\sigma_0-\sigma_1\|\right), \\ y &= \frac{1}{2}\left(\|\sigma_0+\sigma_1\| - \|\sigma_0-\sigma_1\|\right), \\ z &= \frac{1}{2}\left(\|\sigma_2+\sigma_3\| + \|\sigma_2-\sigma_3\|\right), \\ w &= \frac{1}{2}\left(\|\sigma_2+\sigma_3\| - \|\sigma_2-\sigma_3\|\right). \end{aligned} \quad (15)$$

By simple calculations, we can know that the ccq state σ^{ccq}_{ABE} of $|\Psi\rangle_{ABE}$ is

$$\sigma^{ccq}_{ABE} = \frac{1}{2}\sum_{i,j=0}^{1} |ij\rangle\langle ij| \otimes P_{ij}, \quad (16)$$

where P_{00}, P_{11}, P_{01}, and P_{10} are the projections onto the subspaces spanned by $\sqrt{x}|e_0\rangle + \sqrt{y}|e_1\rangle$, $\sqrt{x}|e_0\rangle - \sqrt{y}|e_1\rangle$, $\sqrt{z}|e_2\rangle + \sqrt{w}|e_3\rangle$, and $\sqrt{z}|e_2\rangle - \sqrt{w}|e_3\rangle$, respectively.

We note that one can get $K_D^{DW} = I(A:B) - I(A:E)$ bits of key for the ccq state obtained from the state $|\Psi\rangle_{ABE}$ by Devetak-Winter [5] protocol, where $I(A:B) = S(A) + S(B) - S(AB)$, S being von Neumann entropy. Therefore, by straightforward calculations, one can obtain

$$K_D^{DW}(\sigma^{ccq}_{ABE}) = 1 - S(E), \quad (17)$$

and

$$S(E) = -x\log_2 x - y\log_2 y - z\log_2 z - w\log_2 w. \quad (18)$$

Hence, we obtain the following lemma.

Lemma 2. *Let ρ be a state in $\mathcal{B}(\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^d\otimes\mathbb{C}^d)$ of the form in* Eq. (11)*, and let σ^{ccq}_{ABE} be the ccq state obtained from the privacy squeezed state of ρ. Then $K_D^{DW}(\sigma^{ccq}_{ABE}) = 1 - S(E)$, and furthermore,*

$$S(E) = -x\log_2 x - y\log_2 y - z\log_2 z - w\log_2 w, \quad (19)$$

where x, y, z, and w are in Eq. (15)*.*

We now present another sufficient condition of $K_D > 0$, which is a generalization of a result of Horodecki *et al.* (Proposition 1 in [8]).

Theorem 2. *Let ρ be any state in $\mathcal{B}(\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^d\otimes\mathbb{C}^d)$ with $\rho = \sum_{i,j,k,l=0}^{1} |ij\rangle\langle kl| \otimes A_{ijkl}$, and let*

$$\begin{aligned} x &= (\|A_{0000}\| + \|A_{1111}\|)/2 + \|A_{0011}\|, \\ y &= (\|A_{0000}\| + \|A_{1111}\|)/2 - \|A_{0011}\|, \\ z &= (\|A_{0101}\| + \|A_{1010}\|)/2 + \|A_{0110}\|, \\ w &= (\|A_{0101}\| + \|A_{1010}\|)/2 - \|A_{0110}\|. \end{aligned} \quad (20)$$

If $-x\log_2 x - y\log_2 y - z\log_2 z - w\log_2 w < 1$, then $K_D(\rho) > 0$. More specifically,

$$\begin{aligned} K_D(\rho) \geq 1 &+ x\log_2 x + y\log_2 y \\ &+ z\log_2 z + w\log_2 w > 0. \end{aligned} \quad (21)$$

Proof. ρ has the matrix form

$$\rho = \begin{bmatrix} A_{0000} & A_{0001} & A_{0010} & A_{0011} \\ A_{0100} & A_{0101} & A_{0110} & A_{0111} \\ A_{1000} & A_{1001} & A_{1010} & A_{1011} \\ A_{1100} & A_{1101} & A_{1110} & A_{1111} \end{bmatrix}. \quad (22)$$

If we apply an appropriate twisting operation first, then we can get

$$\rho_{tw} = \begin{bmatrix} B_{0000} & B_{0001} & B_{0010} & B_{0011} \\ B_{0100} & B_{0101} & B_{0110} & B_{0111} \\ B_{1000} & B_{1001} & B_{1010} & B_{1011} \\ B_{1100} & B_{1101} & B_{1110} & B_{1111} \end{bmatrix}, \quad (23)$$

where B_{0000}, B_{1111}, B_{0011}, B_{1100}, B_{0101}, B_{1010}, B_{0110}, and B_{1001} are positive and

$$\begin{aligned} &\mathrm{tr}B_{0000} = \|A_{0000}\|, \quad \mathrm{tr}B_{1111} = \|A_{1111}\|, \\ &\mathrm{tr}B_{0011} = \|A_{0011}\|, \quad \mathrm{tr}B_{1100} = \|A_{1100}\|, \\ &\mathrm{tr}B_{0101} = \|A_{0101}\|, \quad \mathrm{tr}B_{1010} = \|A_{1010}\|, \\ &\mathrm{tr}B_{0110} = \|A_{0110}\|, \quad \mathrm{tr}B_{1001} = \|A_{1001}\|. \end{aligned} \quad (24)$$

By the same LOCC on the subsystem AB as the depolarization in $\mathbb{C}^2\otimes\mathbb{C}^2$, we can get the following state

$$\tilde{\rho}_{tw} = \begin{bmatrix} \frac{B_{0000}+B_{1111}}{2} & 0 & 0 & \frac{B_{0011}+B_{1100}}{2} \\ 0 & \frac{B_{0101}+B_{1010}}{2} & \frac{B_{0110}+B_{1001}}{2} & 0 \\ 0 & \frac{B_{0110}+B_{1001}}{2} & \frac{B_{0101}+B_{1010}}{2} & 0 \\ \frac{B_{0011}+B_{1100}}{2} & 0 & 0 & \frac{B_{0000}+B_{1111}}{2} \end{bmatrix}. \quad (25)$$

Let σ^{tw}_{AB} be the privacy squeezed state of $\tilde{\rho}_{tw}$, and σ^{ccq}_{ABE} be the ccq state obtained from σ^{tw}_{AB}. We remark that the distillable key rate of ρ_{tw} is the same as that of the original state ρ, and furthermore σ^{ccq}_{ABE} has the key rate no better than that of ρ_{tw} [6, 7, 8]. Since $\tilde{\rho}_{tw}$ is of the form in Eq. (11), for x, y, z, and w in Eq. (20), we straightforwardly obtain

$$\begin{aligned} K_D^{DW}(\sigma^{ccq}_{ABE}) &= 1 - S(E) \\ &= 1 + x\log_2 x + y\log_2 y \\ &\quad +z\log_2 z + w\log_2 w, \end{aligned} \quad (26)$$

by Lemma 2. Since $-x\log_2 x - y\log_2 y - z\log_2 z - w\log_2 w < 1$ by our hypothesis, we have

$$K_D(\rho) \geq K_D^{DW}(\sigma^{ccq}_{ABE}) = 1 - S(E) > 0. \quad (27)$$

□

IV. EXAMPLES

We first consider the PPT states with $K_D > 0$ presented in [6, 7].

Example 1. Let $\varrho_s = 2P_{sym}/(d^2+d)$ and $\varrho_a = 2P_{as}/(d^2-d)$ with the symmetric projector P_{sym} and the antisymmetric projector P_{as} on $\mathbb{C}^d \otimes \mathbb{C}^d$, and

$$\rho = \frac{1}{2}\begin{bmatrix} p(\tau_1+\tau_0) & 0 & 0 & p(\tau_1-\tau_0) \\ 0 & (1-2p)\tau_0 & 0 & 0 \\ 0 & 0 & (1-2p)\tau_0 & 0 \\ p(\tau_1-\tau_0) & 0 & 0 & p(\tau_1+\tau_0) \end{bmatrix}, \tag{28}$$

where $\tau_0 = \varrho_s^{\otimes l}$ and $\tau_1 = [(\varrho_a+\varrho_s)/2]^{\otimes l}$. Then we can obtain

$$\rho' = \frac{1}{2^m N}\begin{bmatrix} [p(\tau_1+\tau_0)]^{\otimes m} & 0 & 0 & [p(\tau_1-\tau_0)]^{\otimes m} \\ 0 & [(1-2p)\tau_0]^{\otimes m} & 0 & 0 \\ 0 & 0 & [(1-2p)\tau_0]^{\otimes m} & 0 \\ [p(\tau_1-\tau_0)]^{\otimes m} & 0 & 0 & [p(\tau_1+\tau_0)]^{\otimes m} \end{bmatrix}, \tag{29}$$

with $N = 2p^m + 2(1/2-p)^m$, from ρ by the recurrence protocol. Then it follows from Lemma 3 in Appendix that the state ρ is PPT for $p \in [0, 1/3]$ and $(1-p)/p \geq [d/(d-1)]^l$, and hence the state ρ' is also PPT.

Let

$$\begin{aligned} x &= \frac{1}{2^m N}\left[\|p(\tau_1+\tau_0)\|^m + \|p(\tau_1-\tau_0)\|^m\right] \\ y &= \frac{1}{2^m N}\left[\|p(\tau_1+\tau_0)\|^m - \|p(\tau_1-\tau_0)\|^m\right] \\ z &= w = \frac{1}{2^m N}\|(1-2p)\tau_0\|^m . \end{aligned} \tag{30}$$

Then for $p \in (1/4, 1/3]$, by choosing sufficiently large m and l, we have $-x\log_2 x - y\log_2 y - z\log_2 z - w\log_2 w < 1$. Therefore, we can obtain the PPT states with $K_D > 0$ by Theorem 2.

We consider the low-dimensional PPT states with $K_D > 0$ presented in [8].

Example 2. For two private bits γ_1 and γ_2, take any biased mixture of the form:

$$\rho = p_1\gamma_1 + p_2\sigma_x^A\gamma_2\sigma_x^A \tag{31}$$

with $p_1 > p_2$ and $\sigma_x^A = [\sigma_x]_A \otimes I_{A'BB'}$, where σ_x is one of Pauli matrices representing the bit flip. Then ρ has the following matrix form.

$$\rho = \frac{1}{2}\begin{bmatrix} p_1\sqrt{X_1X_1^\dagger} & 0 & 0 & p_1X_1 \\ 0 & p_2\sqrt{X_2X_2^\dagger} & p_2X_2 & 0 \\ 0 & p_2X_2^\dagger & p_2\sqrt{X_2^\dagger X_2} & 0 \\ p_1X_1^\dagger & 0 & 0 & p_1\sqrt{X_1^\dagger X_1} \end{bmatrix}, \tag{32}$$

where X_1 and X_2 are arbitrary operators with trace norm one. Then we can easily show that the values x, y, z, and w in Theorem 2 are $x = p_1$, $y = 0$, $z = p_2$, and $w = 0$. By Theorem 2, $K_D(\rho) > 0$ since $p_1 + p_2 = 1$ and $p_1 > p_2$.

We present the PPT states with $K_D > 0$ which can be shown by Theorem 1.

Example 3. For $0 < q < (2-\sqrt{2})/8$, let

$$p = \frac{1-2q}{4+2\sqrt{2}}, \tag{33}$$

$$\begin{aligned} \sigma_0 &= p\left(|\phi^+\rangle\langle\phi^+| + |01\rangle\langle 01|\right), \\ \sigma_1 &= p\left(|\phi^-\rangle\langle\phi^-| + |10\rangle\langle 10|\right), \end{aligned} \tag{34}$$

and let Γ denote partial transposition over the subsystem BB'. Then we have $\mathrm{tr}(\sigma_0\sigma_1) = 0$,

$$\begin{aligned} \sigma_0 + \sigma_1 &= p\mathcal{I} = \sigma_0^\Gamma + \sigma_1^\Gamma, \\ \sigma_0 - \sigma_1 &= p\left(|00\rangle\langle 11| + |11\rangle\langle 00| + |01\rangle\langle 01| - |10\rangle\langle 10|\right), \\ (\sigma_0-\sigma_1)^\Gamma &= p\left(|01\rangle\langle 10| + |10\rangle\langle 01| + |01\rangle\langle 01| - |10\rangle\langle 10|\right) \\ &= \sqrt{2}p|\xi_0\rangle\langle\xi_0| - \sqrt{2}p|\xi_1\rangle\langle\xi_1|, \end{aligned} \tag{35}$$

for some orthonormal $|\xi_0\rangle$ and $|\xi_1\rangle$ with

$$|\xi_0\rangle\langle\xi_0| + |\xi_1\rangle\langle\xi_1| = |01\rangle\langle 01| + |10\rangle\langle 10|. \tag{36}$$

Now, let

$$\begin{aligned} \rho &= |\phi^+\rangle\langle\phi^+| \otimes \sigma_0 + |\phi^-\rangle\langle\phi^-| \otimes \sigma_1 \\ &\quad + |\psi^+\rangle\langle\psi^+| \otimes \sigma_2 + |\psi^-\rangle\langle\psi^-| \otimes \sigma_3, \end{aligned} \tag{37}$$

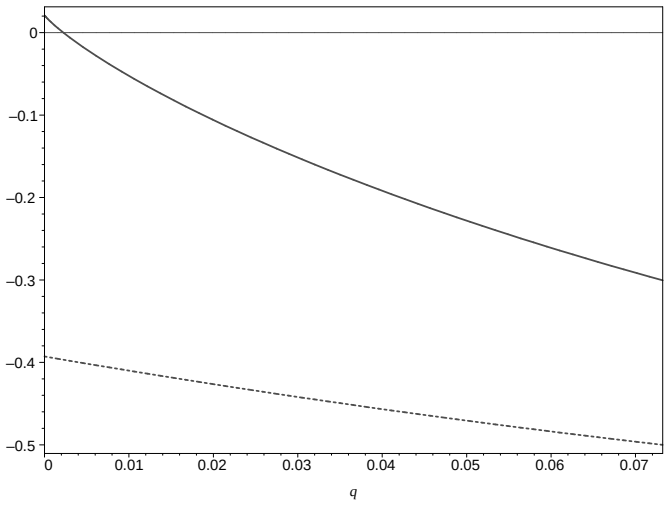

FIG. 1: The values of K_D^{DW} for the ccq states of the privacy squeezed states: The solid and dashed curves represent the values of K_D^{DW} for the ccq states of their privacy squeezed states in Example 3 and Example 4, respectively.

where

$$\begin{aligned}\sigma_2 &= \sqrt{2}p|\xi_0\rangle\langle\xi_0| + q|00\rangle\langle 00|,\\ \sigma_3 &= \sqrt{2}p|\xi_1\rangle\langle\xi_1| + q|00\rangle\langle 00|. \end{aligned} \quad (38)$$

Then $\|\sigma_0 - \sigma_1\| = 4p > 1/2$, and it follows from Corollary 1 that $K_D(\rho) > 0$.

Since

$$\begin{aligned}\sigma_2 - \sigma_3 &= (\sigma_0 - \sigma_1)^\Gamma,\\ \sigma_2 + \sigma_3 &= \sqrt{2}p\,(|\xi_0\rangle\langle\xi_0| + |\xi_1\rangle\langle\xi_1|) + 2q|00\rangle\langle 00|\\ &= \sqrt{2}p\,(|01\rangle\langle 01| + |10\rangle\langle 10|) + 2q|00\rangle\langle 00|\\ &= (\sigma_2 + \sigma_3)^\Gamma, \end{aligned} \quad (39)$$

$\rho^\Gamma = \rho$, that is, ρ has PPT. Therefore, ρ's are the PPT states with positive distillable key.

However, since the values x, y, z, and w in Theorem 2 are $x = 4p$, $y = 0$, $z = 2\sqrt{2}p + q$, and $w = q$,

$$\begin{aligned}K_D^{DW}(\sigma_{ABE}^{ccq}) &= 1 + 4p\log_2 4p + q\log_2 q\\ &\quad +(2\sqrt{2}p + q)\log_2(2\sqrt{2}p + q) \end{aligned} \quad (40)$$

is not always positive for $0 < q < (2-\sqrt{2})/8$ as seen in Fig. 1, where σ_{ABE}^{ccq} is the ccq state for the privacy squeezed state of ρ. Therefore, when $K_D^{DW} < 0$, by means of Theorem 2, one cannot determine whether ρ has positive distillable key rate or not, although one can readily show that $K_D(\rho) > 0$ by Corollary 1.

We now present another PPT states with $K_D > 0$ but $K_D^{DW} < 0$ for the ccq states of their privacy squeezed states.

Example 4. Let

$$\varrho = \frac{1}{2}\begin{bmatrix} \sigma_0+\sigma_1 & 0 & 0 & \sigma_0-\sigma_1 \\ 0 & 2\sigma_2 & 0 & 0 \\ 0 & 0 & 2\sigma_2 & 0 \\ \sigma_0-\sigma_1 & 0 & 0 & \sigma_0+\sigma_1 \end{bmatrix}, \quad (41)$$

where

$$\begin{aligned}\sigma_0 &= p(|\phi^+\rangle\langle\phi^+| + |01\rangle\langle 01|),\\ \sigma_1 &= p(|\phi^-\rangle\langle\phi^-| + |10\rangle\langle 10|),\\ \sigma_2 &= \frac{p}{\sqrt{2}}(|01\rangle\langle 01| + |10\rangle\langle 10|)\\ &\quad +\frac{q}{2}|00\rangle\langle 00| + \frac{q}{2}|11\rangle\langle 11|, \end{aligned} \quad (42)$$

with $p = (1-2q)/(4+2\sqrt{2})$ for $0 \le q < (2-\sqrt{2})/8$. Then since

$$\varrho^\Gamma = \frac{1}{2}\begin{bmatrix} \sigma_0^\Gamma+\sigma_1^\Gamma & 0 & 0 & 0 \\ 0 & 2\sigma_2^\Gamma & \sigma_0^\Gamma-\sigma_1^\Gamma & 0 \\ 0 & \sigma_0^\Gamma-\sigma_1^\Gamma & 2\sigma_2^\Gamma & 0 \\ 0 & 0 & 0 & \sigma_0^\Gamma+\sigma_1^\Gamma \end{bmatrix}, \quad (43)$$

and $2\sigma_2^\Gamma \pm (\sigma_0^\Gamma - \sigma_1^\Gamma)$ is positive, ϱ is a PPT state by Lemma 3 in Appendix. Since ϱ satisfies all conditions of Theorem 1, and therefore $K_D(\varrho) > 0$.

However, as in Example 3, we can see that $K_D^{DW} < 0$ for the ccq states of their privacy squeezed states. More precisely, one can obtain that

$$\begin{aligned}K_D^{DW} &= 1 + 4p\log_2 4p\\ &\quad +2(\sqrt{2}p + q)\log_2(\sqrt{2}p + q) \end{aligned} \quad (44)$$

is negative for all $0 \le q < (2-\sqrt{2})/8$, as seen in Fig. 1.

V. SUMMARY

We have investigated properties of quantum states with positive distillable key rate, and have constructed sufficient conditions for states to have positive distillable key rate. Exploiting the conditions, we have shown that the PPT bound entangled states given by Horodecki *et al.* [6, 7, 8] have nonzero distillable key rate, and have exhibited a new class of PPT bound entangled states with $K_D > 0$, but with $K_D^{DW} < 0$ for the ccq states of their privacy squeezed versions.

Acknowledgments

D.P.C. was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. R01-2006-000-10698-0), and S.L. was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2006-003-C00044).

APPENDIX: SIMPLE LEMMAS

In this appendix, we present some simple but useful lemmas.

Lemma 3. *Let A and B be $n \times n$ hermitian matrices. Then $\begin{bmatrix} A & B \\ B & A \end{bmatrix}$ is positive if and only if $A \pm B$ is positive.*

Proof. Let $\mathbf{x}$ and $\mathbf{y}$ be any vector in $\mathbb{C}^n$. Then we have

$$\begin{aligned} & \begin{bmatrix} \mathbf{x}^\dagger & \mathbf{y}^\dagger \end{bmatrix} \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix} \\ = \; & \mathbf{x}^\dagger A \mathbf{x} + \mathbf{y}^\dagger A \mathbf{y} + \mathbf{x}^\dagger B \mathbf{y} + \mathbf{y}^\dagger B \mathbf{x} \\ = \; & \frac{1}{2}(\mathbf{x}^\dagger + \mathbf{y}^\dagger)(A+B)(\mathbf{x}+\mathbf{y}) \\ & + \frac{1}{2}(\mathbf{x}^\dagger - \mathbf{y}^\dagger)(A-B)(\mathbf{x}-\mathbf{y}). \end{aligned} \tag{A.1}$$

Therefore, we can clearly obtain the proof of this lemma from Eq. (A.1). □

Lemma 4. *For any two positive operators σ_0 and σ_1, $\|\sigma_0 - \sigma_1\| = \|\sigma_0 + \sigma_1\|$ if and only if $\mathrm{tr}(\sigma_0\sigma_1) = 0$.*

Proof. If $\mathrm{tr}(\sigma_0\sigma_1) = 0$, then it is trivial that $\|\sigma_0 - \sigma_1\| = \|\sigma_0 + \sigma_1\|$. We now assume that $\|\sigma_0 - \sigma_1\| = \|\sigma_0 + \sigma_1\|$. Note that there exist positive operators τ_0 and τ_1 such that $\sigma_0 - \sigma_1 = \tau_0 - \tau_1$ and $\mathrm{tr}(\tau_0\tau_1) = 0$. Then from the following equalities

$$\begin{aligned} \mathrm{tr}(\sigma_0) - \mathrm{tr}(\sigma_1) &= \mathrm{tr}(\sigma_0 - \sigma_1) = \mathrm{tr}(\tau_0 - \tau_1) \\ &= \mathrm{tr}(\tau_0) - \mathrm{tr}(\tau_1), \end{aligned} \tag{A.2}$$

and

$$\begin{aligned} \mathrm{tr}(\sigma_0) + \mathrm{tr}(\sigma_1) &= \|\sigma_0 + \sigma_1\| = \|\sigma_0 - \sigma_1\| = \|\tau_0 - \tau_1\| \\ &= \mathrm{tr}(\tau_0) + \mathrm{tr}(\tau_1), \end{aligned} \tag{A.3}$$

we obtain $\mathrm{tr}(\sigma_0) = \mathrm{tr}(\tau_0)$ and $\mathrm{tr}(\sigma_1) = \mathrm{tr}(\tau_1)$. Since $\mathrm{tr}(\tau_0\tau_1) = 0$, there exist two disjoint index sets I_0, I_1, and an orthonomal basis $\{|x_j\rangle : j \in I_0 \cup I_1\}$ such that $\tau_0 = \sum_{j\in I_0} \lambda_j |x_j\rangle\langle x_j|$ and $\tau_1 = \sum_{j\in I_1} \lambda_j |x_j\rangle\langle x_j|$ for some $\lambda_j \geq 0$. Then it is straightforwad to have the following equalities.

$$\begin{aligned} \sum_{j\in I_0} \langle x_j|\sigma_0|x_j\rangle \; - \; & \sum_{j\in I_0} \langle x_j|\sigma_1|x_j\rangle \\ = \; & \sum_{j\in I_0} \langle x_j|\sigma_0 - \sigma_1|x_j\rangle = \sum_{j\in I_0} \langle x_j|\tau_0 - \tau_1|x_j\rangle \\ = \; & \sum_{j\in I_0} \langle x_j|\tau_0|x_j\rangle - \sum_{j\in I_0} \langle x_j|\tau_1|x_j\rangle \\ = \; & \sum_{j\in I_0} \langle x_j|\tau_0|x_j\rangle = \sum_{j\in I_0\cup I_1} \langle x_j|\tau_0|x_j\rangle \\ = \; & \mathrm{tr}(\tau_0) = \mathrm{tr}(\sigma_0) \\ = \; & \sum_{j\in I_0} \langle x_j|\sigma_0|x_j\rangle + \sum_{j\in I_1} \langle x_j|\sigma_0|x_j\rangle. \end{aligned} \tag{A.4}$$

Hence, we obtain

$$\sum_{j\in I_1} \langle x_j|\sigma_0|x_j\rangle + \sum_{j\in I_0} \langle x_j|\sigma_1|x_j\rangle = 0. \tag{A.5}$$

Since σ_0 and σ_1 are positive, it can be obtained that $\langle x_j|\sigma_0|x_j\rangle = 0$ for any $j \in I_1$, and $\langle x_j|\sigma_1|x_j\rangle = 0$ for any $j \in I_0$. Therefore, we conclude that $\mathrm{tr}(\sigma_0\sigma_1) = 0$. □

Now, we consider the recurrence protocol [10] to distill a pbit [6, 7]. By simple but tedious calculations, we obtain the following lemma.

Lemma 5 (Recurrence protocol)**.** *For any states ρ_1 and ρ_2 in $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \otimes \mathbb{C}^d)$, let*

$$\rho_1 = \begin{bmatrix} A_{0000} & A_{0001} & A_{0010} & A_{0011} \\ A_{0100} & A_{0101} & A_{0110} & A_{0111} \\ A_{1000} & A_{1001} & A_{1010} & A_{1011} \\ A_{1100} & A_{1101} & A_{1110} & A_{1111} \end{bmatrix}, \tag{A.6}$$

and

$$\rho_2 = \begin{bmatrix} B_{0000} & B_{0001} & B_{0010} & B_{0011} \\ B_{0100} & B_{0101} & B_{0110} & B_{0111} \\ B_{1000} & B_{1001} & B_{1010} & B_{1011} \\ B_{1100} & B_{1101} & B_{1110} & B_{1111} \end{bmatrix}. \tag{A.7}$$

After some LOCC operations in the recurrence protocol, $\rho_1 \otimes \rho_2$ can be transformed into a state in $\mathcal{B}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d^2} \otimes \mathbb{C}^{d^2})$. Let ρ_{jj} be the resulting state when the measurement outcome is jj. Then we have

$$\rho_{00} = \frac{1}{N_0}\begin{bmatrix} A_{0000}\otimes B_{0000} & A_{0001}\otimes B_{0001} & A_{0010}\otimes B_{0010} & A_{0011}\otimes B_{0011} \\ A_{0100}\otimes B_{0100} & A_{0101}\otimes B_{0101} & A_{0110}\otimes B_{0110} & A_{0111}\otimes B_{0111} \\ A_{1000}\otimes B_{1000} & A_{1001}\otimes B_{1001} & A_{1010}\otimes B_{1010} & A_{1011}\otimes B_{1011} \\ A_{1100}\otimes B_{1100} & A_{1101}\otimes B_{1101} & A_{1110}\otimes B_{1110} & A_{1111}\otimes B_{1111} \end{bmatrix},$$

$$\rho_{11} = \frac{1}{N_1}\begin{bmatrix} A_{0000}\otimes B_{1111} & A_{0001}\otimes B_{1110} & A_{0010}\otimes B_{1101} & A_{0011}\otimes B_{1100} \\ A_{0100}\otimes B_{1011} & A_{0101}\otimes B_{1010} & A_{0110}\otimes B_{1001} & A_{0111}\otimes B_{1000} \\ A_{1000}\otimes B_{0111} & A_{1001}\otimes B_{0110} & A_{1010}\otimes B_{0101} & A_{1011}\otimes B_{0100} \\ A_{1100}\otimes B_{0011} & A_{1101}\otimes B_{0010} & A_{1110}\otimes B_{0001} & A_{1111}\otimes B_{0000} \end{bmatrix}, \tag{A.8}$$

where

$$N_0 = \sum_{j,k=0}^{1} \|A_{jkjk}\| \cdot \|B_{jkjk}\|, \tag{A.9}$$

and

$$N_1 = \sum_{j,k=0}^{1} \|A_{jkjk}\| \cdot \|B_{\bar{j}\bar{k}\bar{j}\bar{k}}\|, \tag{A.10}$$

with $\bar{j} = j + 1 \pmod 2$.

[1] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[2] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[3] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
[4] L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
[5] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0506189.
[8] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, quant-ph/0506203.
[9] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, quant-ph/0608199.
[10] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).